

FILED
LODGED
ENTERED
RECEIVED
AO 106 (Rev. 04/10) Application for a Search Warrant (Modified: WAWD 10-26-18)

NOV 08 2019

UNITED STATES DISTRICT COURT

AT SEATTLE
CLERK U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
BY DEPUTY

for the
Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
Email account grizzled@protonmail.com stored at
premises controlled by Paxful, Inc.

Case No. MJ19-547

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Email account grizzled@protonmail.com stored at premises controlled by Paxful, Inc., more fully described in Attachment A,

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
Title 18, U.S.C. § 1343
Title 18, U.S.C. § 1956 & 1957

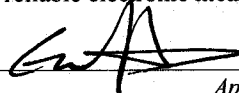
Offense Description
Wire Fraud
Money Laundering

The application is based on these facts:

- ☒ See Affidavit of Special Agent Eric Hergert, continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☐ by reliable electronic means; or: ☐ telephonically recorded.



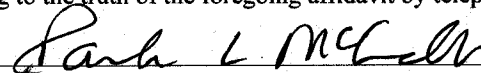
Applicant's signature

Eric Hergert, IRS Special Agent

Printed name and title

- ☒ The foregoing affidavit was sworn to before me and signed in my presence, or
☐ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 11/08/2019



Judge's signature

City and state: Seattle, Washington

Paula L. McCandlis United States Magistrate Judge

Printed name and title

INTRODUCTION AND AGENT BACKGROUND

2. I earned a Bachelor of Arts degree in accounting from the University of Washington, Tacoma, in 2002. I attended the Criminal Investigator Training Program and the IRS Special Agent Basic Training at the Federal Law Enforcement Training Center (FLETC) where I received detailed training in conducting financial investigations. The training included search and seizure, the Internal Revenue laws, and IRS procedures and policies in criminal investigations. I have also attended various cybercrime and virtual currency related trainings, including at FLETC and others.

4. I have conducted and assisted in numerous investigations involving financial crimes. I have led and participated in the execution of search warrants and have

1 interviewed witnesses and defendants who were involved in, or had knowledge of,
2 violations of the Internal Revenue Code, the Bank Secrecy Act, and the Money
3 Laundering Control Act. In the course of my employment with IRS-CI, I have conducted
4 and have been involved in investigations of alleged criminal violations, which have
5 included tax evasion (26 U.S.C. § 7201), filing a false tax return (26 U.S.C. § 7206(1)),
6 aiding or assisting in the preparation of false tax returns (26 U.S.C. § 7206(2)),
7 conspiring to defraud the United States (18 U.S.C. § 371), wire and mail fraud (18 U.S.C.
8 §§ 1343, 1341), aggravated identity theft (18 U.S.C. § 1028A), and money laundering (18
9 U.S.C. §§ 1956, 1957), among others.

10 5. I have led and participated in the execution of federal search warrants and
11 the consensual searches of records relating to the concealment of assets and proceeds
12 derived from fraud. These records included, but were not limited to, email accounts,
13 instant messages, personal telephone books, photographs, bank records, escrow records,
14 credit card records, tax returns, business books and records, and computer hardware and
15 software.

16 6. I also have specialized training in cryptocurrencies, with a focus on Bitcoin
17 and Ethereum. This has included training into how publically viewable “blockchains”
18 record cryptocurrency transactions, how to trace funds through these transactions,
19 attribution techniques used to identify individuals responsible for conducting the
20 transactions; and methods used by individuals to obfuscate the source of, or their control
21 over, cryptocurrencies. I have used these techniques in prior and ongoing investigations.
22 Additionally, I have conducted cryptocurrency training for others, both internal to the
23 IRS, as well as for external third parties.

24 7. The facts set forth in this Affidavit are based on my own personal
25 knowledge; knowledge obtained from other individuals during my participation in this
26 investigation, including other law enforcement officers; review of documents and records
27 related to this investigation; communications with others who have personal knowledge
28

1 of the events and circumstances described herein; and information gained through my
2 training and experience.

3 **PLACES TO BE SEARCHED AND ITEMS TO BE SEIZED**

4 8. I make this affidavit in support of an application for a search warrant for
5 information associated with the www.paxful.com ("Paxful") account registered under the
6 email address grizzled[]protonmail.com (the "SUBJECT ACCOUNT").¹ Paxful is a
7 web-based cryptocurrency exchange, which offers (among other services) an electronic
8 communications service that permits the website's users to communicate with each other
9 about the purchase and sale of cryptocurrency and other topics (referred to on Paxful and
10 herein as "trade chats"). According to Paxful representatives, Paxful keeps a record of
11 trade chats conducted on its platform, and such chats can include messages about the gift-
12 card codes and other forms of currency that users exchange for cryptocurrency. Paxful is
13 headquartered at 3422 Old Capitol Trail #989, Wilmington, DE, 19808

14 9. The information to be searched is described in the following paragraphs
15 and in Attachment A. This affidavit is made in support of an application for a search
16 warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Paxful
17 to disclose to the government copies of the information, including the content of
18 communications, further described in Section I of Attachment B. Upon receipt of the
19 information described in Section I of Attachment B, government-authorized persons will
20 review that information to locate the items described in Section II of Attachment B.

21 10. The facts set forth in this Affidavit are based on my own personal
22 knowledge; knowledge obtained from other individuals during my participation in this
23 investigation, including other law-enforcement personnel; review of documents and
24 records related to this investigation; communications with others who have personal
25 knowledge of the events and circumstances described herein; and information gained
26

27
28 ¹ I have bracketed a portion of the SUBJECT ACCOUNT's registered email address to ensure that it is not
inadvertently hyperlinked and contacted by anyone reading an electronic copy of this document.

1 through my training and experience. Because this Affidavit is submitted for the limited
2 purpose of establishing probable cause in support of the application for a search warrant,
3 it does not set forth each and every fact that I or others have learned during the course of
4 this investigation.

5 11. Based on my training and experience and the facts as set forth in this
6 Affidavit, there is probable cause to believe that violations of Title 18, United States
7 Code, Section 1343 (Wire Fraud), and Title 18, United States Code, Sections 1956 and
8 1957 (Money Laundering) have been committed by known and unknown persons. There
9 is also probable cause to search the SUBJECT ACCOUNT, as described in Attachment
10 A, for evidence, instrumentalities, contraband, or fruits of these crimes, as described in
11 Attachment B.

12 SUMMARY OF THE INVESTIGATION

13 12. As detailed in the sections below, IRS and the United States Secret Service
14 ("Secret Service") have investigated VOLODYMYR KVASHUK ("KVASHUK") for
15 devising and executing a scheme to defraud Microsoft Corporation ("Microsoft").
16 KVASHUK is presently charged in the case of *United States v. Kvashuk*, CR19-143JLR,
17 which is presently pending in the United States District Court for the Western District of
18 Washington. As described in the Indictment in that case, KVASHUK worked for
19 Microsoft and was assigned to develop and test the company's online retail sales
20 platform. In that role, KVASHUK was supposed to make simulated purchases of
21 Microsoft products from the company's online store. The testing system was designed to
22 ensure that no physical products would be shipped. KVASHUK, however, used test
23 accounts to purchase massive amounts of "currency stored value," or "CSV," such as
24 digital gift cards. The investigation has shown that KVASHUK, in his role as a tester,
25 made unauthorized purchases of millions of dollars of CSV, which he then resold on the
26 Internet. KVASHUK used the proceeds of the fraud to purchase, among other things, a
27 \$160,000 Tesla car and a \$1.6 million home in Renton, Washington.

1 13. As part of this investigation, I have obtained records from numerous
2 sources, met with counsel for Microsoft, interviewed Microsoft employees, and
3 conducted search warrants at KVASHK's residence and on various email accounts
4 associated with the scheme.

5 Microsoft's Program To Test Online Retail Sales

6 14. Microsoft has given me a copy of KVASHUK's resume which shows that
7 he is a Seattle-based software engineer. According to information provided by Microsoft,
8 KVASHUK was an employee of a Microsoft vendor. As part of his employment with the
9 vendor, KVASHUK worked on matters for Microsoft from August 26, 2016, until
10 October 1, 2017. During that time, KVASHUK worked out of Microsoft's office and had
11 access to the company's computer network. On December 1, 2017, Microsoft hired
12 KVASHUK as a full-time employee with an annual salary of approximately \$116,000.
13 KVASHUK worked for Microsoft until June 22, 2018.

14 15. Microsoft sells various products to the general public over the Internet via
15 its online store. To make purchases from the Microsoft store, a customer must establish a
16 Microsoft store account that is linked to an email address and to one or more payment
17 devices (such as a credit card). As both an employee of an outside vendor, and as a
18 Microsoft employee, KVASHUK was a member of Microsoft's Universal Store Team
19 ("UST"), which supports the company's online retail platform, by (among other things)
20 managing a program that tests the online sales system.

21 16. The testing program involves creating test Microsoft store accounts that are
22 linked to test email accounts created specifically for the purpose of the testing program.
23 A tester creates a test email account by using a naming convention for the account: the
24 name begins with "mstest," followed by an underscore and, in the typical case, the user
25 name of the tester. The tester then requests that the UST team "whitelist" the account,
26 meaning that purchases made from the account will automatically bypass Microsoft's
27 security and risk protocols, which monitor online purchases in order to detect possible
28 fraud. The test accounts are linked to artificial payment devices ("Test in Production" or

1 “TIP” cards) – in effect, phony credit cards – that allow the tester to simulate a purchase
2 without generating an actual charge. Once the whitelisted account is created, the tester
3 uses that account to attempt to make online product purchases from Microsoft, just as an
4 ordinary consumer would.

5 17. According to Microsoft investigators, although each test account was
6 created for a particular tester, the login and password information for some of the test
7 accounts may have been stored in an electronic document that was accessible to multiple
8 testers. Microsoft investigators told me that, in practice, testers sometimes used test
9 accounts set up for other testers. However, during recent interviews, current and former
10 UST members have stated that they were unaware of a particular document with login
11 and password information, and that they were unaware of testers using other testers’
12 accounts. These UST members have stated that login and password information may
13 have been accessible in other ways.

14 18. According to Microsoft, the testing program primarily was designed to test
15 the company’s online sales of physical goods. When a tester used a whitelisted account
16 to purchase physical goods, the system ensured that no goods were actually delivered.

17 19. UST members have stated that there was some, limited, testing that
18 involved simulated purchases of electronic currency stored value (“CSV”), such as digital
19 gift cards. If a tester did purchase CSV, the system would generate a valid and usable
20 product “key” that could be “redeemed,” meaning that the value of the digital currency
21 would be added to an electronic “wallet” linked to a customer account. Once redeemed,
22 the CSV could be used to buy both physical and digital products from the Microsoft
23 store.

24 20. According to Microsoft employees I have interviewed, there are occasional
25 circumstances which could warrant a tester to purchase CSV with their test accounts.
26 However, this was a relatively rare occurrence, and only small amounts of CSV would be
27 purchased (\$5-\$10). Additionally, testers could be provided access to a pool of “test”
28

1 CSV codes to be used for testing certain features, eliminating the need to purchase CSV
2 with their test accounts.

3 The Theft Of \$10 Million In Microsoft's Digital Currency

4 21. According to information provided by Microsoft, in February of 2018,
5 Microsoft's UST Fraud Investigation Strike Team ("FIST") noticed a suspicious increase
6 in the use of CSV to buy subscriptions to Microsoft's Xbox live gaming system from
7 Microsoft's online store. FIST investigated and discovered that the suspicious CSV had
8 originally been purchased from Microsoft through two whitelisted test accounts
9 associated with the email accounts mstest_avestu@outlook.com and
10 mstest_sfwe2eauto@outlook.com (the "avestu" and "sfwe2eauto" test accounts). The
11 CSV was then resold on the secondary market, at a discount, via at least three online
12 reseller websites: Paxful, g2a.com, and nokeys.com. Customers who purchased the CSV
13 on the secondary market then redeemed the CSV at Microsoft's online store for products
14 and services, such as Xbox live subscriptions.

15 22. FIST discovered that the avestu and swfe2eauto test accounts were used to
16 buy a large amount of CSV between November 2017 and March 2018. The avestu and
17 swfe2eauto accounts were blocked by Microsoft on or about March 15, 2018. FIST later
18 discovered that a third test account linked to mstest_zabeerj2@outlook.com (the
19 "zabeerj2" test account) was also responsible for a suspicious spike in CSV purchases,
20 conducting approximately 166 purchases of CSV between March 22 and March 23, 2018.
21 This account was blocked on or about March 23, 2019.

22 23. The employees who had registered the accounts at issue have explained the
23 accounts were used for production testing. However, the
24 mstest_sfwe2eauto@outlook.com account was used for automated testing, and the
25 username and password were stored in a Visual Studio project file, accessible by several
26 Microsoft employees. Additionally, usernames and passwords of the test accounts were
27 often captured by logging software used to assist in the identification and correction of
28

software bugs. Reports from the logging software, including the usernames and passwords were routinely provided to developers, including KVASHUK.

24. The three suspicious test accounts were used to purchase roughly \$10.1 million in CSV from Microsoft. Microsoft was able to “blacklist” roughly \$1.8 million in CSV to prevent it from being redeemed, resulting in a total loss to Microsoft of approximately \$8.3 million.

CSV Redemptions by Acquisition Account

Account	2017	2018	Total
Mstest_avestu	\$357,595.00	\$1,298,010.00	\$1,655,605.00
Mstest_swfe2eauto	\$601,261.27	\$5,444,340.04	\$6,045,601.31
Mstest_zabeerj2	\$0.00	\$643,380.00	\$643,380.00
Total	\$958,856.27	\$7,385,730.04	\$8,344,586.31

25. Microsoft interviewed the employees who created the three suspicious test accounts and found no evidence that they were involved in the fraudulent CSV purchases.

26. A search of KVASHUK’s computer and digital devices found the usernames and passwords for the test accounts in various files. Also found in these files were Internet links to webpages on the Microsoft online store. The username and password were for the zabeerj2 account were found in a custom program designed to automate the purchase of CSV from the Microsoft online store. This program was last modified March 21, 2018, shortly after the avestu and swfe2eauto accounts were blocked, and immediately prior to the zabeerj2 account being used in the scheme.

27. Searches of KVASHUK’s computer and other digital devices also found several screenshots, text files, and spreadsheets that contained large amounts of what appear to be CSV codes. A few of these codes were provided to Microsoft and were verified to have been acquired through the use of the test accounts described above.

1 28. Microsoft investigators also found similar CSV acquisitions by the test
2 account mstest_v-vokvas@outlook.com (the “vokvas” test account), though on a much
3 smaller scale. This account was created by, and assigned to, KVASHUK.

4 29. Microsoft records show that the vokvas test account made purchases of
5 CSV on April 28, July 10, September 29, October 4, October 7, October 11, and October
6 22 of 2017. The amount of CSV obtained through the vokvas account totaled
7 approximately \$12,304.99, of which approximately \$4,464.99 was redeemed.²
8 According to Microsoft records, KVASHUK’s vokvas test account was used to purchase
9 approximately \$10,164.99 in CSV in October 2017, after KVASHUK’s employment with
10 the Microsoft vendor ended and before being employed by Microsoft.

11 30. According to Microsoft records, approximately \$600 of the CSV purchased
12 by the vokvas account was redeemed to a Microsoft store account linked to the email
13 address safirion@outlook.com (the “safirion” account).

14 31. Microsoft investigators interviewed KVASHUK on May 10 and May 18 of
15 2018. Although no law enforcement officer was at those interviews, I have listened to
16 recordings of the interviews. The interviews were not completely recorded because of a
17 technical problem, but I have also read summaries of the interviews and spoken with
18 Microsoft investigator Andy Cookson, who was present at both interviews.

19 32. The interviewers asked KVASHUK about the purchases made with the
20 vokvas test account. KVASHUK admitted that he had created the vokvas account. He
21 also admitted to making some unauthorized purchases from the account. KVASHUK
22 suggested that there was a lack of guidance from his superiors about what could and
23 could not be purchased via a test account, and claimed to have only been told that test
24 accounts should not be used to purchase subscriptions. KVASHUK admitted to
25 Microsoft investigators the safirion account was his personal account, and that he used
26

27 ² Approximately \$100 of the redeemed CSV appears to have been in Canadian currency. It was not possible to
28 determine from the records available how much of the \$12,304.99 in CSV obtained through the vokvas account
was in a foreign currency.

1 CSV acquired through his vokvas test account to buy movies from the Microsoft store.
2 KVASHUK claimed that he believed it was permissible to use test accounts to buy CSV
3 because it was not “real” money.

4 33. According to Microsoft records, additional redemptions of the CSV
5 acquired through the vokvas account were only redeemed to Microsoft online store
6 accounts associated with the email addresses admin@searchdom.io,
7 xidijenizo@axsup.net, or pikimajado@tinzoa.org until November 22, 2017. Through the
8 course of the investigation, all of these email accounts have been linked to KVASHUK .

9 a. Searchdom.io is the Internet domain name associated with the
10 business Searchdom, Inc. According to Washington Secretary of State records,
11 KVASHUK is a “governor” of the business. Additionally, the Microsoft online store
12 account associated with the email address admin@searchdom.io is registered to “Volo
13 kvashuk,” and lists one of KVASHUK’s previous addresses.

14 b. xidinenizo@axsup.net and pikimajado@tinzoa.org appear to be a
15 temporary email addresses. These email addresses and apparent passwords were found in
16 various files during a search of KVASHUK’s computer and digital devices pursuant to a
17 search warrant conducted July 16, 2019.

18 34. According to records obtained from Google, on November 22, 2017, at
19 approximately 12:17 PM, KVASHUK conducted an internet search for “cash in xbox
20 gift.” Then, KVASHUK immediately visited the website, gameflip.com. Gameflip.com
21 advertises that it allows users to list Xbox Live gift cards for sale on their site. After a
22 gift card is purchased by a customer, Gameflip.com deposits the proceeds into the seller’s
23 “gameflip wallet.” The seller can then withdraw the proceeds “any time into your
24 PayPal, bank account, or Bitcoin.”

25 35. Subsequently, on November 22, 2017, at approximately 7:48 PM, \$50
26 Canadian of CSV acquired through the vokvas account was redeemed to an unknown
27 individual’s Microsoft store account associated with the email address
28 sunmoon94@hotmail.ca. Over the next few days, approximately 12 more redemptions of

1 CSV acquired by the vokvas account totaling approximately \$1,150 (\$50 of which were
 2 Canadian) were made to Microsoft store accounts associated with email addresses with
 3 no known connection to KVASHUK. Based on this information, it appears he began
 4 selling the CSV through third party websites on or about November 22, 2017.

5 36. The SUBJECT ACCOUNT began buying bitcoin using Xbox gift cards as
 6 payment on November 23, 2017. Between November 23, 2017 and March 26, 2018, over
 7 447 bitcoin was purchased through Paxful.com by this account using Xbox gift cards as
 8 the payment method. The value of the Xbox gift cards used to purchase the bitcoin was
 9 approximately \$7.88 million.³

10 The email address used to register the SUBJECT ACCOUNT,
 11 grizzled[@]protonmail.com, is linked to KVASHUK. More specifically,
 12 grizzled[@]protonmail.com was associated with an account at Coinbase.com registered
 13 to KVASHUK. In addition, a search of KVASHUK's computer found various references
 14 to grizzled[@]protonmail.com, including a list of account recovery codes, and the
 15 Windows username of what appeared to be the primary account was named "grizzled."

16 Evidence of Unexplained Wealth

17 37. Financial records show that KVASHUK had a large amount of unexplained
 18 income during the period of the CSV thefts. According to his tax returns for 2016 and
 19 2017, KVASHUK only had total income of \$35,260 and \$114,103, respectively.
 20 According to Microsoft, for the portion of time KVASHUK was a direct employee
 21 (December 2017 to June 2018), his annual salary was \$116,000.

22
 23
 24 ³ Bitcoin is a form of virtual currency (also known as cryptocurrency), a digital representation of value that can be
 25 exchanged directly person to person, through a virtual currency exchange, or through other intermediaries. It can be
 26 used to buy goods and services, exchanged for fiat currency or other virtual currency, or held as an investment,
 27 among other applications. Virtual currency is generally not issued by any government or bank. Rather, it is often
 28 generated and controlled through software operating on a decentralized, peer-to-peer network of computers across
 the world. The U.S.-dollar exchange value of an individual unit of bitcoin is variable and subject to market forces.
 For instance, during the time period November 23, 2017 and March 26, 2018, the U.S. dollar value of individual
 units of bitcoin varied within the general range of approximately \$6,600 per unit of bitcoin to approximately
 \$19,100 per unit of bitcoin.

1 38. KVASHUK used his unexplained wealth to make significant purchases.
2 In March of 2018, KVASHUK paid roughly \$162,000 for a Tesla Model S. Additionally,
3 in June of 2018, KVASHUK bought a lakeside home in Renton, Washington for roughly
4 \$1.675 million. Both of these purchases were completely funded directly from accounts
5 controlled by KVASHUK.

6 39. I have reviewed records for a checking account that KVASHUK had at
7 Wells Fargo bank, ending in -5789. The earliest daily balance shown on the records was
8 \$429.56 on July 29, 2016. The balance on the account remained under \$20,000 until late
9 November of 2017, when large amounts of money from a cryptocurrency account in
10 KVASHUK's name at Coinbase.com began to flow into the -5789 account. On
11 November 30, 2017, over \$14,000 was transferred to the -5789 account from
12 Coinbase.com. On December 11, 2017, over \$6,600 was transferred from Coinbase.com
13 to the -5789 account. On December 21, 2017, there was a transfer of over \$29,000 from
14 Coinbase.com to the -5789 account.

15 40. The suspicious transfers escalated dramatically in early 2018. For example,
16 on January 30th, February 2nd, and February 6th of 2018, there were transfers from
17 Coinbase of over \$98,000, \$177,000 and \$134,000, respectively. On a single day –
18 March 2, 2018 – over \$500,000 was transferred from Coinbase to the -5789 account.
19 Over \$1.4 million was transferred in total in March 2018, followed by over \$935,000 in
20 April.

21 41. All told, over \$2.8 million was transferred from Coinbase to the -5789
22 account between November 2017 and May 2018. The approximate timeframe of the vast
23 majority of the fraud was November 2017 through March 2018. Given these timeframes,
24 and based on my training and experience, it appears that KVASHUK had converted the
25 proceeds of the fraud into cryptocurrency (or received the proceeds as cryptocurrency),
26 and then gradually converted the cryptocurrency in fiat currency and transferred the
27 proceeds to his Wells Fargo account.
28

1 42. Furthermore, in order to determine the source of the cryptocurrency
2 “bitcoin” in the Coinbase account, I have examined the bitcoin blockchain, a public
3 ledger of bitcoin transactions. Based on this analysis, it appears the vast majority of the
4 bitcoin deposited into the Coinbase account originated from chipmixer.com.
5 Chipmixer.com is a bitcoin “mixing” service. A bitcoin mixing service mixes potentially
6 identifiable bitcoin with others, with the intent to obscure and conceal the original source
7 of the bitcoin. Based on my training and experience, the use of chipmixer.com is
8 evidence of an attempt to conceal proceeds of the fraud.

9 43. In addition to the bitcoin sourced from chipmixer.com, I was able to trace a
10 deposit of 1.5 bitcoin into KVASHUK’s Coinbase account on November 29, 2017 as
11 having come directly from the SUBJECT ACCOUNT. According to records produced
12 by Paxful, the SUBJECT ACCOUNT purchased over 447 bitcoin between November
13 2017 and March 2018 by using Xbox gift cards as the payment method. My analysis of
14 bitcoin being withdrawn from the SUBJECT ACCOUNT found many instances of the
15 bitcoin being deposited into what appears to be bitcoin addresses associated with
16 chipmixer.com. In other words, in addition to the direct deposits from the SUBJECT
17 ACCOUNT into KVASHUK’s Coinbase account, the SUBJECT ACCOUNT also made
18 direct deposits into chipmixer.com, which (as explained above) subsequently transferred
19 bitcoin into KVASHUK’s Coinbase account.

20 **PROBABLE CAUSE REGARDING THE PLACES TO BE SEARCHED**

21 44. As explained above, Paxful representatives have informed me that Paxful
22 permits users on its platform to buy and sell bitcoin. For instance, the Paxful website
23 informs prospective users that they can “buy and sell bitcoin using over 300 payment
24 options,” including “bank transfers,” “cash,” “debit/credit cards,” other “digital
25 currencies,” and (as relevant to this case) “gift cards.” According to Paxful
26 representatives, Paxful enables users to communicate with each other over a proprietary
27 messaging platform that Paxful operates, with the ostensible goal of negotiating the
28 purchase and sale of bitcoin using one of the payment options that Paxful supports.

1 Paxful refers to these communications between users as “trade chats.” As Paxful
2 representatives have explained to me, trade chats often include information such as the
3 gift-card numbers that are being used to purchase bitcoin.

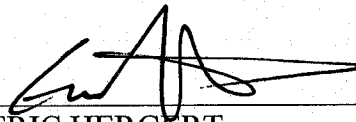
4 45. For the reasons set out above, I respectfully submit that there is probable
5 cause to believe that the SUBJECT ACCOUNT’s trade chats will contain evidence of the
6 crimes under investigation. In light of the evidence that KVASHUK purchased bitcoin
7 on Paxful, his trade chats with other users on Paxful are likely to contain evidence of the
8 precise means that he used to purchase that bitcoin, including the stolen CSV that he
9 exchanged for the bitcoin that he eventually transferred into his Coinbase account.

10 //

11 //

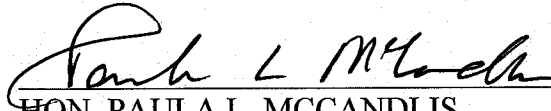
CONCLUSION

46. Based on the foregoing, I respectfully request that the Court issue the proposed search warrant. More specifically, by this Affidavit and Warrant I seek authority for the government to search all of the items specified in Section I, Attachment B (attached hereto and incorporated by reference herein) to the Warrant, and specifically to seize all of the data, documents and records that are identified in Section II to the same Attachment.



ERIC HERGERT
Special Agent,
Internal Revenue Service

SUBSCRIBED and SWORN to before me this 8th day of November, 2019.



HON. PAULA L. MCCANDLIS
United States Magistrate Judge

ATTACHMENT A

Account to be Searched

The electronically stored data, information, and communications, subscriber records, and log records contained in, related to, and associated with (including all preserved data) the Paxful, Inc. account registered under the email address grizzled@protonmail.com ("SUBJECT ACCOUNT"), which is stored at premises controlled by Paxful, Inc., an electronic communications service provider headquartered at 3422 Old Capitol Trail #989, Wilmington, DE, 19808.

ATTACHMENT B

I. Section I - Information to be disclosed by Paxful, Inc., for search:

To the extent that the information described in Attachment A is within the possession, custody, or control of Paxful, Inc. ("Paxful"), regardless of whether such information is located within or outside the United States, including any electronic messages, records, files, logs, or information that has been deleted but is still available to Paxful, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(d), Paxful is required to disclose the following information to the government for the account listed in Attachment A:

- a. The contents of all "trade chats", user messages, or other forms of communication associated with the account, including stored or preserved copies of communication sent to and from the account, the source and destination addresses or accounts associated with each communication, and the date and time at which each communication was sent;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, forwarding email addresses, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records pertaining to communications between Paxful and any person regarding the account, including contacts with support services and records of actions taken.
- e. All records available regarding the location of the user of the account, including information obtained from IP addresses, GPS, or wifi access points;
- f. All records regarding device-specific information for devices used to access the accounts, including hardware model, operating system, unique device identifiers, and mobile network information, including phone numbers; and

1 g. Records of any other accounts associated with the account through common
2 cookies, device identifiers, email addresses, or phone numbers.
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

II. Section II - Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of Wire Fraud, in violation of Title 18, United States Code, Section 1343, and Money Laundering, in violation of Title 18, United States Code, Sections 1956 and 1957, including the following (for the time period January 1, 2017 to the present):

- a. Communications, or material related to the actual or attempted transfer, resale, or redemption of Microsoft currency stored value, digital currency, gift cards, or subscriptions;
- b. Communications or material related to online resellers of gift cards, CSV, or bitcoin;
- c. Communications or material related the possible transfer or disposition of the proceeds of the fraud, including: to accounts at banks or other financial institutions; financial transactions or transfers; the purchase, transfer or sale of cryptocurrency; the use of the proceeds of the fraud to buy real property, vehicles, or goods or services; and any explanations, reports, or other information regarding the amount and sources of funds or other income;
- d. All messages, documents, and profile information, attachments, or other data that serves to identify any persons who use or access the account specified, or who exercise in any way any dominion or control over the specified account;
- e. All messages, documents and profile information, attachments, or other data that otherwise constitutes evidence, fruits, or instrumentalities of violations of Wire Fraud, in violation of Title 18, United States Code, Section 1343, and Money Laundering, in violation of Title 18, United States Code, Sections 1956(a)(1) and 1957.
- f. All subscriber associated with the specified account, including name, address, local and long distance telephone connection records, or records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment for such service) including any credit card or bank account number;

1 g. Any records of communications between Paxful, and any person about issues
2 relating to the account, such as technical problems, billing inquiries, or complaints
3 from other users about the specified account. This to include records of contacts
4 between the subscriber and the Paxful's support services, as well as records of any
5 actions taken by the Paxful or subscriber as a result of the communications.
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28